UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/053,013	01/18/2002	David Kammer	035451-0170 (3708.Palm)	2103

26371 7590 02/10/2009

FOLEY & LARDNER LLP
777 EAST WISCONSIN AVENUE
MILWAUKEE, WI 53202-5306

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
02/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/053,013	KAMMER ET AL.	
	Examiner	Art Unit	
	SHANTO M. ABEDIN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25 and 27-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25 and 27-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/31/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the communication filed on 11/11/2008.

2. Claims 1-25 and 27-53 are pending inn the application.

3. Claims 1-25 and 27-53 are rejected.

Response to Arguments

4. The applicant's arguments regarding the previous 35 USC 103 (a) type rejections are fully considered, however, found not persuasive. Regarding the previous 35 USC 103(a) type rejections the applicant primarily argues that the cited references Stewart, or Bade independently or in combination fails to disclose the method wherein the determined location and the security protection for the network user node are updated continuously. However, the examiner respectfully disagrees with the applicant. Upon further examination, reference Stewart et al was found teach the method wherein the determined location and the security protection for the network user node are updated continuously (Col 5, starts at line 22, Col 7, lines 5-29; Col 8, line 26-43; access levels are determined/ updated based on the current geographical locations). Furthermore, reference Bade et al was found to teach the method wherein the determined location and the security protection for the network user node are updated continuously (Fig 3.316; Col 3, starts at line 55; Col 4, lines 30-54; dynamically setting the security parameters based on the positional data). Although the examiner believes that the combination of the cited references teaches, or at least suggest enablement of the claimed invention, for the sake of the arguments/ response, the examiner incorporates a newly found reference Hastings et al that clearly teaches continuous update of the determined location and the security protection for the network user node (Col 4, line 35- Col 5, line 30; updating security policy, encryption parameters for each time period).

5. The applicant's arguments regarding 35 USC 103(a) type rejections of claims 17, 29 and 49 further in view of Rusch are fully considered, however, moot in view of new grounds of rejections presented in this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-25 and 27-53 are rejected under 35 USC 103 (a) as being unpatentable over Stewart et al (US 6970927 B1) in view of Bade et al (US 6,778,837 B2) further in view of Hastings et al (US 6370629 B1)

Regarding claim 1, Stewart et al teaches a method of adjusting security for a network user node in a communication with network based upon the location of the node, comprising:

determining the location of a network user node (Col 8, lines 26-42; Col 20, lines 1-10; determining geographic location of the portable computing device) ;

selecting a single level of security from a group of more than two security levels based on the determined location (Fig 5; access levels associated with the plurality of destination location information; Col 8, lines 26-42; provide services to the user based on geographic location information; Col 19, lines 60-67; Col 20, lines 1-10; access level is determined based on geographic location), the group of more than two security levels being stored in the memory (Col 6, lines 10-30; supporting multiple access levels; Col 20, lines 25-59; storing first, second access levels); and

modifying the security protection for the network user node based upon the selected level of security (Col 20, lines 25-59; modifying/ switching to first or second access levels depending on location; wherein the access level is stored in a memory; Col 7, lines 5-25; Col 10, lines 24-40; Col 20, lines 1-35; access level is based on geographic location; providing network access to the portable computing device based on the access level);

wherein the group of more than two security levels is defined (Col 3, lines 15-28; Col 8, lines 44-50; Col 10, line 65 to Col 11, lines 3; the access information may be provided by the PCD of the user; access level is based on geographic location);

wherein the determined location and the security protection for the network user node are updated continuously (Col 5, starts at line 22, Col 7, lines 5-29; Col 8, line 26-43; access levels are determined/ updated based on the current geographical locations).

Stewart et al fails to teach expressly security levels being stored in the network user node; and wherein the group/ security level is defined by a user of the network user node.

However, Bade et al teaches security levels being stored in the network user node (Fig 2; Col 3, lines 35- Col 4, line 28; storing predefined access parameter set by the user); and wherein the group/ security level is defined by a user of the network user node (Col 3, lines 35- Col 4, line 28; Col 6, lines 20-45; user setting access parameters). Bade et al further teaches wherein the determined location and the security protection for the network user node are updated continuously (Fig 3.316; Col 3, starts at line 55; Col 4, lines 30-54; dynamically setting the security parameters based on the positional data).

Alternatively, Hastings et al teaches wherein the determined location and the security protection for the network user node are updated continuously (Col 4, line 35- Col 5, line 60; updating security policy, encryption parameters for each time period).

Hastings et al , Bade et al and Stewart et al are analogous art because they are from the same field of endeavor of using geographic/ physical location information for providing access security/ authentication in a wireless network system. At the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teaching of Hastings et al with the modified Bade et al-Stewart et al method to further include security levels being stored in the memory of the network user node, and wherein the group of more than two security levels is defined by a user of the network user node in order to provide users with the control of the security system dynamically.

Regarding claim 18, it is rejected applying as same motivation and rationale applied above rejecting claim 1, furthermore, Stewart et al teaches a computer system for modifying security settings for a network user node based on the location of the node comprising:

an input device having a communicative coupling with a system for determining the location of a network user node (Col 8, lines 26-40; PCD may include a GPS equipment to enable the PCD to provide its geographic location);

a storage device (Col 14, lines 39-55; Col 5, lines 35-55; PCD memory) for storing a table of security modification to be performed based on a plurality of locations for the network user node, the security modification including more than two levels (Col 20, lines 25-59; modifying/ switching to first or second access levels depending on location; wherein the access level is stored in a memory comprised in a portable computing device);

a processor coupled to a storage device for processing information,(Col 5, lines 50-67; PCD with wireless Ethernet card; Col 21, lines 60-67; Col 22, lines 1-10; determine the access level for the portable computing device by accessing the memory medium); and

a communication device capable of transmitting a data signal to the network user node (Col 7, lines 5-25; Col 8, lines 26-40);

wherein the determined location and the security protection for the network user node are updated continuously (Col 5, starts at line 22, Col 7, lines 5-29; Col 8, line 26-43; access levels are determined/ updated based on the current geographical locations).

Stewart et al fails to teach the security modification is defined by a user of the network user node; storing on a storage device, and generating a security modification instruction; and the network user node containing instructions to modify the security protection for the node.

However, Bade et al teaches the security modification is defined by a user of the network user node. (Col 3, lines 35- Col 4, line 28; Col 6, lines 20-45; user setting access parameters); storing on a storage device, and generating a security modification instruction (Fig 2; Col 3, lines 35- 60; Col 4, line 1-67; storing in authentication module/ software for setting predefined access parameter by the user); and the network user node containing instructions to modify the security protection for the node (Col 3, lines 35- 60; Col 4, line 1-67; authentication module/ software; automatically, dynamically changing access parameter). Bade et al further teaches wherein the determined location and the security protection for the network user node are updated continuously (Fig 3.316; Col 3, starts at line 55; Col 4, lines 30-54; dynamically setting the security parameters based on the positional data).

Alternatively, Hastings et al teaches wherein the determined location and the security protection for the network user node are updated continuously (Col 4, line 35- Col 5, line 60; updating security policy, encryption parameters for each time period).

Regarding claims 30 and 38, they recite the limitations of claims 1 and 18, therefore, they are rejected applying as same motivation and rationale above applied rejecting claims 1 and 18.

Regarding claim 2, it is rejected applying as same motivation and rationale applied above rejecting claim 1, furthermore, Stewart et al teaches network user node is a mobile device having a display (Col 5, lines 59-67; Col 6, lines 1-10; portable computing device/ PCD, PDA).

Regarding claim 3, it is rejected applying as above rejecting claim1, furthermore, Stewart et al teaches the network user node's location is determined using a location sensing system (Col 8, lines 26-40; PCD may include a GPS equipment to enable the PCD to provide its geographic location).

Regarding claim 4, it is rejected applying as above rejecting claim 3, furthermore, Stewart et al teaches the location sensing system is a global positioning satellite (GPS) system (Col 8, lines 26-40; PCD may include a GPS equipment to enable the PCD to provide its geographic location).

Regarding claim 5, it is rejected applying as above rejecting claim 3, furthermore, Stewart et al teaches location sensing system uses signal bouncing and triangulation to determine network user node location (Col 2, lines 8-16; wireless network comprising Access Points, AP; Col 8, lines 26-42; providing geographic locations information of PCD).

Regarding claim 6, it is rejected applying as above rejecting claim 3, furthermore, Stewart et al discloses location sensing system to determine network user node location (Col 8, lines 26-40; PCD may include a GPS equipment to enable the PCD to provide its geographic location). Stewart et al fails to disclose the use of signal bouncing and triangulation for that purpose.

However, Bade et al discloses the use of signal bouncing and triangulation to determine network user node location (Col 3, starts at line 20; triangulation).

Regarding claim 7, it is rejected applying as above rejecting claim 3, furthermore, Stewart et al teaches network user node is in direct communication with the location sensing system (Col 8, lines 26-42).

Regarding claim 8, it is rejected applying as above rejecting claim 1, furthermore, Stewart et al teaches sending a data signal includes transmitting the data signal using a wireless local area network (WLAN) protocol (Col 10, lines 1-25, 55-67;wireless LAN).

Regarding claim 9, it is rejected applying as above rejecting claim 8, furthermore, Stewart et al teaches WLAN protocol includes the IEEE 802.11 protocol (Col 10, lines 1-25, 55-67; IEEE 802.11; wireless LAN).

Regarding claim 10, it is rejected applying as above rejecting claims 6 and 8, furthermore, Bade et al discloses WLAN protocol includes Bluetooth wireless network protocol (Col 3, starts at line 35; cellular/ wireless transceiver). Although Bade et al does not expressly teach a bluetooth protocol, since at the time of invention, Bluetooth technology was

well known in the art, it would be logically obvious to a person of ordinary skill in the art to use Bluetooth as wireless/ cellular protocol to provide an alternative cellular protocol.

Regarding claim 11, it is rejected applying as above rejecting claim 1, furthermore, Stewart et al teaches the selecting step is carried out by reference to a table of desired security modifications based upon the location of network user node (Fig 5, element: table of identification information and associated access information; Col 7, lines 30-67; table comprising identification and access control information).

Regarding claim 12, it is rejected applying as above rejecting claim 11 furthermore, Stewart et al teaches security levels are provided by the user of the network user node for a variety of locations (Col 19, lines 60-67; Col 20, lines 1-20; Col 21, lines 10-40; Col 23, lines 45-50; plurality of access points; plurality of network portable devices).

Regarding claim 13, it is rejected applying as above rejecting claim 11 furthermore, Stewart et al teaches the security level is based on the type of location determined for the network user node (Fig 5, element : identification information comprising plurality of access levels associated with the plurality of destination location information; Col 8, lines 26-42; provide services to the user based on geographic location information; Col 19, lines 60-67; Col 20, lines 1-10; access level is determined based on geographic location).

Regarding claim 14, it is rejected applying as above rejecting claims 1 and 6, furthermore, Stewart et al discloses the step of modifying the security protection for the

network user node includes restricting access to information unless a password is properly entered (Col 2, starting at line 20; Col 7, lines 5-25; access control).

Furthermore, Bade et al discloses restricting access to information unless a password is properly entered (Col 4, starting at line 47).

Regarding claim 15, it is rejected applying as above rejecting claim 1, furthermore, Stewart et al teaches the step of modifying the security protection for the network user node includes a complete denial of access to information using the network user node (Fig 4, element 226: disallowing access; Col 20, lines 5-35; if the access level is the second access level, the data is not provided).

Regarding claim 16, it is rejected applying as above rejecting claim 1, furthermore, Stewart et al teaches denial to a subset of the information accessible using the node (Col 7, lines 5-30; Col 20, lines 5-35; providing appropriate level of access; providing access to one or more resources depending on permission level).

Regarding claim 17, it is rejected applying as above rejecting claims 1, furthermore, Stewart et al discloses modifying the security protection for the network user node on data transmitted by the network user node (Col 20, lines 25-59; modifying access levels depending on location). Modified Bade et al-Stewart et al method fails to disclose modifying data encryption parameters to change the strength of encryption on data.

However, Hastings et al discloses modifying data encryption parameters to change strength of encryption on data (Col 3, lines 35-65; Col 4, starts at line 42; change of encryption level, and parameter or key depending of the geographic regions).

Regarding claims 19 -25, 27-28, 37, 42 and 45, they recite the limitations of claims 1-9, 10-14, 18, 30 and 38, therefore, they are rejected applying as above rejecting claims 1-9, 10-14, 18, 30 and 38.

Regarding claims 29, 31-36, 39-41, 43-44, and 46-49, they recite the limitations of claims 1 -9, 11-13, 17-18 and 38, therefore, they are rejected applying as above rejecting claims 1-9, 11-13, 17-18 and 38.

Regarding claims 50-53, they recite the limitations of claim 1,18,30, 38, therefore, they are rejected applying as above rejecting claim 1,18,30 and 38, furthermore, Stewart et al teaches network user node is a portable handheld device (Col 5, lines 59-67; Col 6, lines 1-10; portable computing device/ PCD, PDA).

Conclusion

7. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195.

The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436